Summary of the activities of the ERNCIP Applied Biometrics for security of CI Thematic Group

Sylvia Yang
Danish Institute of Fire and Security Technology (DBI)

March 2015

The research leading to these results has received funding from the European Union as part of the European Reference Network for Critical Infrastructure Protection project.

Report EUR 27208 EN

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Georgios Giannopoulos
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 721, 21027 Ispra (VA), Italy
E-mail: erncip-office@jrc.ec.europa.eu
Tel.: +39 0332 78 6211
Fax: +39 0332 78 5469

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC95665

EUR 27208 EN

ISBN 978-92-79-47752-2

ISSN 1831-9424

doi:10.2788/409925

Luxembourg: Publications Office of the European Union, 2015

Printed in Italy

Table of Contents

1. General description of the Thematic Group

Purpose

Biometric identity technology, such as fingerprint, iris or face recognition, is foreseen to become more and more common for access control to critical infrastructure and for travel documents. Test and evaluation presents challenges of scale because the required correct identification rates are often high and the acceptable false alarm rate low, so very many test data records must be run to determine the performance.

There are also issues of privacy and data protection to consider.
The reliability of biometric technologies is unknown. In particular the following criteria are often unknown or impossible to compare against competitors:

- The performance of the underlying biometric system
- The robustness to vulnerabilities such as direct (spoofing) or indirect attacks, and
- The strength of privacy preservation techniques.

The lack of standard operational evaluations is the reason that we cannot measure the reliability of these biometric technologies. Some initiatives exist in Europe, the USA, and Asia. However, these initiatives are: isolated (focusing only on one or two biometric modalities), disorganised, or limited in time (very few are organising on-going evaluations). This leads to discontinuous and non-integrated efforts which have a limited life span.

Thus there is a need for establishing a framework to evaluate, in a systematic way, the performance of biometric technologies using several metrics and criteria (performance, vulnerability, privacy).

Objectives

Two principle objectives were identified:

- to develop resources to highlight the appropriate use of biometric technologies and systems in application to critical infrastructure protection, and
- to contribute to the standardisation, evaluation, testing and certification initiatives in key application areas.

Group structure

Coordinator: Marek Rejman-Greene, Home Office Centre for Applied Science and Technology (CAST), UK

Participating organisations (Jan 2015):

CH	Idiap Research Institute (former Institut Dalle Molle d'Intelligence Artificielle Perceptive)
DE	Fraunhofer Insitute for Computer Graphics Research
DE	Cognitec
DE	Secunet
DE	BSI
DK	DBI
ES	Universidad Carlos III
FR	Safran Morpho
NL	European Biometrics Group
PL	Government Centre for Security
PL	Naukowa i Akademicka Sieć Komputerowa (Research and Academic Computer Network)/Warsaw University of Technology
UK	Home Office Centre for Applied Science and Technology
UK	Ministry of Defence
UK	CESG (former Communications-Electronics Security Group)
UK	National Physical Laboratory
UK	IBM
UK	University of Surrey

The members of the Group met nine times between December 2012 and January 2015.

2. Way of working

The TG decided to split its work into a number of tasks, organised under two broad work package headings, namely:

1. Work on awareness, elicitation of priorities, promotion of appropriate use of biometrics in CIs
2. Standardisation, evaluation, testing and certification to meet the requirements of operators of CIs and other stakeholders.

In particular, the Group identified the following applications where biometrics can support security processes:

- Automated Border Controls
- Physical access control (particularly to special zones within a restricted area of operation of critical infrastructure)
- Logical access control (Additional security for access to IT systems)
- Mobile identity checks ('on-the-spot challenge'/virtual zones in restricted areas of operation of critical infrastructures)
- Biometric recognition of individuals from CCTV (link to TG on Video Analytics and Surveillance).

3. Results and Deliverables 2011-2014

The main achievements of the Group were the consolidation of input to:

- ISO/IEC JTC 1/SC 17 Technical Committee for Biometric Standards, regarding Biometrics in CCTV (see below)
- CEN Technical Committee 224 Working Group 18 – Biometrics, regarding Biometrics for physical access control (see below)

During 2014, TG members contributed to a new work item (multipart standard ISO/IEC 30137) which was proposed and accepted by SC37 for development on biometric CCTV activities, and to a new work item for standards development on biometric physical access control activities. In addition, reports were produced by the Group on:

- Experiences from Large Scale Testing of Systems using Biometric Technologies[1]
- The Application of Biometrics in Critical Infrastructures Operations: Guidance for Security Managers[2] .

ISO/IEC JTC 1/SC 17 Technical Committee for Biometric Standards, regarding Biometrics in CCTV

At the January 2014 plenary meeting of JTC1 ISO/IEC SC37 (The international standards subcommittee on biometrics), a New Work Item was adopted on *Use of operator-assisted automated face recognition in CCTV systems* having gained the required number of votes from national standardisation bodies. The ERNCIP Thematic Group contributed significantly to the development of one of the base documents which complemented the submission from the South Korean national standards body. Discussion on the scope of the new three part standard resulted in a change of name to *Use of biometrics in Video surveillance systems*. Work on the three parts of the standard has continued at the Working Group meetings of SC37 in July 2014 (West Lafayette, Indiana, USA) and in January 2015 (Toledo, Spain).

[1] Published JRC nnnnn
[2] Published JRC nnnnn

The current status of the three parts of the standard, ISO/IEC 30137, is summarised in the following table:

Part number and title of standard	**Part 1** Design and specification	**Part 2** Performance testing and reporting	**Part 3** Data formats
SC37 working group number and title	WG4 (Technical Implementation of Biometric Systems)	WG5 (Biometric Performance Testing and Reporting)	WG3 (Biometric Data Interchange Formats)
Most recent document	SC37 WG4 N17 (Base Document)	SC37 WG5N0027 (First Working Draft)	SC37 WG 3 N 0089 (First Working Draft)
Editor	Geoff Whitaker*	Hakil Kim	Patrick Grother (interim)
Co-Editors	Marek Rejman-Greene* Shashi Samprathi Sebastien Brangoulo	Tony Mansfield* Marek Rejman-Greene*	Elham Tabassi Geoff Whitaker*

* Editors and Co-editors with asterisks are members of the ERNCIP Thematic Group on Applied Biometrics.

The scope statements are due to be aligned at a future meeting of SC37, but are currently:

Scope of 30137 - Part 1: Design and specification

This multi-part standard is applicable to the use of biometrics in video surveillance systems (also known as Closed Circuit Television or CCTV systems) for a number of scenarios, including real-time operation against watchlists and in post event analysis of video data.

The standard:

- defines the key terms for use in the specification and testing of AFR in video surveillance systems, including metrics for defining performance
- provides guidance on selection of camera types, placement of cameras, image specification, etc., for operation of a face recognition capability
- provides guidance on the composition of the gallery (which may be a blacklist or a whitelist) against which face images from the video surveillance system are compared, including the selection of appropriate images of sufficient quality, and the size of the watchlist in relation to performance requirements
- makes recommendations on data formats for facial images and other relevant information (including metadata) obtained from video footage, used in watchlist images, or from observations made by human operators
- establishes general principles for supporting the operator of the video surveillance system, including user interfaces and processes to ensure

efficient and effective operation and the requirements for trained and motivated personnel
- establishes best practice in supporting the operator, e.g. user interfaces and processes to ensure efficient and effective operation of the system and the requirements for trained and motivated personnel
- specifies performance metrics and testing methodologies applicable to performance measurement of operational systems (addressing the nature of video, with multiple frames and multiple individuals, as well as the use of the operator in determining the final outcome)
- establishes a governance processes to address requirements for security, as well as the requirements for privacy and personal data protection specific to the use of AFR in video surveillance applications (e.g. internationally recognizable signage), and societal considerations in the deployment of systems

This multi-part standard is primarily applicable to the use of Automated Face Recognition (AFR) in video surveillance systems for a number of use cases and scenarios of operation.
Examples include real-time operation against watchlists and post event analysis of video data.

The standard also supports (through an informative annex) related recognition and detection tasks in video surveillance systems such as:
- estimation of crowd densities
- determining patterns of movement of individuals
- identification of individuals appearing in more than one camera
- use of other biometric modalities such as gait or iris recognition
- use of specialized software to infer attributes of individuals, e.g., estimation of gender and age
- interfaces to other related functionality, such as video analytics for behaviour to measure
- queue lengths or alerting for abandoned baggage

Scope of 30137 - Part 2: Performance testing and reporting

This standard:
- describes a framework for testing and reporting the performance of detecting and recognizing humans in the video captured by a surveillance camera which is in general installed relatively far from the human, compared to traditional biometric systems
- defines the key terms for use in the specification and testing of automated face recognition and other biometric recognition in video surveillance systems, including metrics defining performance
- specifies testing methodologies applicable to performance measurement of operational systems (addressing the nature of video, with multiple frames and

multiple individuals, as well as the use of the operator in determining the final outcome)
- specifies requirements on test methods, recording of data, and reporting of results.

Not within the scope of this part of 30137 are:
- Evaluation of human adjudicators

Scope of 30137 - Part 3: Data formats

This part of ISO/IEC 30137 specifies data format(s) for storing, recording and transmitting biometric information acquired via a CCTV system. It is anticipated that in most cases the biometric modality will be face, but this standard is not restricted solely to face image data (for example it may be possible to extract iris images in some scenarios where high resolution cameras are used.

CEN Technical Committee 224 Working Group 18 – Biometrics, regarding Biometrics for physical access control

The ERNCIP Thematic Group on Applied Biometrics supported the response to European Commission's Mandate M/487 to establish a Roadmap for Security Standards, in working with the Netherlands Standardisation Institute in Phase 2, in one of the three priority sectors, *Border security – common technical and interoperability standards for automated border control systems, as well as standards for biometric identifiers*. Marek Rejman-Greene attended the workshop organised in Frontex' premises in Warsaw on 4-5 April 2013, and the ERNCIP group reviewed the documents emerging from Phase 2. The Co-ordinator also attended workshops on approaches to common security accreditation of Automated Border Controls held at JRC Ispra.

4. Expected future focus

The activities initiated with ISO and CEN for Biometric CCTV and for physical access control will need to be continued in 2015 in order to reach the objective of developed standards in 2016. In addition, it is being planned to consult with stakeholders on their areas of concern around European norms for data privacy and biometrics that are being challenged by current and proposed implementations of systems using biometric data.

European Commission
EUR 27208 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: Summary of the activities of the ERNCIP Applied Biometrics for security of CI Thematic Group

Author: Sylvia Yang, Danish Institute of Fire and Security Technology (DBI)

2015 – 13 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-47752-2

doi:10.2788/409925

Abstract

Biometric identity technology, such as fingerprint, iris or face recognition, is foreseen to become more and more common for access control to critical infrastructure and for travel documents. Test and evaluation presents challenges of scale because the required correct identification rates are often high and the acceptable false alarm rate low, so very many test data records must be run to determine the performance.

LB-NA-27208-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

doi:10.2788/409925

ISBN 978-92-79-47752-2

Publications Office